ACET

DATA PROTECTION POLICY

DOCUMENT CONTROL		POLICY LEVEL	
APPROVED BY	Trust Board level	APROVED DATE	April 2024
BUSINESS LEAD	DPO	AUTHOR	Rachel Denton
NEXT REVIEW DATE	March 2025	FREQUENCY	Annually
VERSION NUMBER	DATE ISSUED	UPDATED INFORMATION	
2.0	March 2024	Actions to minimise impact of data breaches – Page 15. And minor changes to retention schedule appendix 1	

1) Statement of intent

Aston Community Education Trust (ACET) is required to keep and process certain information about its staff members, pupils, parents/carers, governors, visitors and other individuals in accordance with its legal obligations under the 2018 General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018).

ACET may, from time to time, be required to share personal information about its staff or pupils with other organisations, as required for business and safeguarding purposes.

This policy is in place to ensure all staff are aware of their responsibilities and outlines how ACET and its academies comply with the following core principles of GDPR.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2) Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3) Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4) The data controller

Our trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5) Roles and responsibilities

This policy applies to all staff employed by our trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1) Trust strategic board

The Trust Strategic Board has overall responsibility for ensuring that our academies comply with all relevant data protection obligations.

5.2) Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Strategic Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

5.3) CEO and Principals

The CEO and Principals acts as the representative of the data controller on a day-to-day basis.

5.4) All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school/trust of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

6) Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7) Collecting personal data

7.1) Lawfulness, fairness and transparency

ACET will only process personal data where we have one or more 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions.
- The data needs to be processed for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, ACET will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If any academy offers online services to pupils, such as classroom apps, we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2) Limitation, minimisation and accuracy

ACET will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Data Retention Policy.

8) Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law

9) Subject access requests and other rights of individuals

9.1) Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, by either letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2) Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our primary academies may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3) Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee that takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4) Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10) Parental requests to see educational records

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil). The principal of the academy should be contacted in the first instance.

11) CCTV

ACET uses CCTV in various locations around the academy sites to ensure it remains safe.

We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12) Photographs and videos

As part of our academy activities, we may take photographs and record images of individuals within our academies.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within the academies on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages.
- Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13) Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing privacy impact assessments where processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our academy and DPO and all information we are required to share about how we use and process their personal data.
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

14) Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

15) Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

We will retain records in accordance with the '*Retention Guidelines for Schools'* produced by the Records Management Society. (*Please see appendix 1)*

16) Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17) Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out below.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.
- High risk personal information such as medical records and financial information.

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the principals and the chair of governors and where appropriate the CEO and chair of directors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality

    - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically on the trust's secure drive
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours.
- The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the trust's secure drive.

- The DPO and principal/CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. We will offer refresher GDPR training to all ACET staff.

Appendix 1

Summary guidelines of records retention periods for schools

Please Note:

Due to the ongoing Independent Inquiry into Child Sexual Abuse (IICSA) no pupil and staff record should be destroyed until further notice. The guidance below gives a retention period (in the 'Retention Action' column), but where records should **not be** destroyed, this has been noted in the 'Disposal Action' column.

SCHOOL RETENTION GUIDELINES

Introduction

These guidelines have been produced by ACET to assist schools in the management of their records. The guidelines outline the recommended retention periods for schools based on legislation and common practice.

It is the responsibility of Academies to retain their records for the appropriate retention period, or to transfer their historical records (those specifically highlighted in this document) to ACET Record Department. The retention guidelines produced in this document are some of the key retention periods which need to be considered. For a comprehensive list of retention periods schools should consult the Schools Toolkit produced by the Information and Records Management Society available at https://irms.org.uk/page/SchoolsToolkit

Explanatory Notes

The retention guidelines will outline a description of records, followed by the action to be taken in (e.g. retain for 3 years). This will be based on an event/action which will trigger that retention action (e.g. date record created). The disposal action will either be the destruction of the records, or their transfer to the ACET Academy Record store
These guidelines may include references to records which are no longer routinely created as part of school business (e.g. log books). These have been included to assist schools who have a large backlog of historical records which require reviewing.

Under the Freedom of Information Act 2000. LA schools (including schools which are granted academy status) are regarded as public bodies and are subject to the Act. This requires that schools manage their records appropriately against agreed retention periods.

Glossary of Terms:

Business decision: if there is no law or regulation to say how long a record should be kept, we may base this decision on the administrative needs of ACET.

Closure: when a record ceases to be 'current' – this can be the when a set of minutes are formally agreed, or when a Help Desk incident is formally closed. Many retention periods are triggered after the 'closure' of a record.

Common practice: if there is no law or regulation to say how long a record should be kept, we may base this decision on what similar organisations do.

Disposal: the processes associated with the end of a records lifecycle, they will typically include destruction of the records or transfer of the records to ACET Record Office for permanent preservation

Functional Description: the description of the function that the record serves (i.e. the functional description of a set of minutes is 'the process of preparing business…')

Permanent: Retain the record permanently and offer to ACET Record Office

Record: the recorded evidence about an activity

Retention Action: the action regarding the retention of a record, triggered by a particular event (e.g. closure of a record)

For further information about the contents of this retention schedule, or for records management generally contact the Data Controller at datacontroller@astoncetrust.org

Ref	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
CHILD PROTECTION						
SCH 1.1	Child protection files (primary school)	Retain for the duration of the pupil's attendance at the school	Date pupil changes school	Transfer to Secondary School	Keeping Children Safe in Education (Department for Education)	Where a child is removed from the roll to be educated at home/missing from education see below
SCH 1.2	Child protection files (secondary school)	Retain for 25 years	Pupil's date of birth	**Do not** destroy (refer to note on front page) Consider transfer to off- site storage on child reaching school leaving age	"Safeguarding Children in Education" 2004 Keeping Children Safe in Education (Department for Education)	Where a child is removed from the roll to be educated at home/missing from education see below

SCH 1.3	Child protection files (Child missing from education, Traveler, Roma, and therefore removed from roll)	Retain for 25 years (as above)	Date removed from roll	Transfer to ACET Record Office	"Safeguarding Children in Education" 2004 Keeping Children Safe in Education (Department for Education)	Scan all your documents into one folder and send via the Secure Portal

SCH 1.4	Child protection files (child is removed from the roll and is Elective Home Educated)	Retain for 25 years (as above)	Date removed from roll	Transfer to ACET Record Office	"Safeguarding Children in Education" 2004 Keeping Children Safe in Education (Department for Education)	Scan all your documents into one folder and send via the Secure Portal
SCH 1.5	Allegations of a child protection nature made against a member of staff (including unfounded allegations)	Retain until the normal retirement age for the member of staff or for 10 years (whichever is the longer)	Employee's retirement age	**Do not** destroy (refer to note on front page)	Employment Practices Code: Supplementary Guidance (Information Commissioner's Office)	
GOVERNORS						
SCH 2.1	Principal set of signed minutes	Retain at school for 6 years	Date of meeting	Transfer to ACET Record	Common practice	
SCH 2.2	Inspection copies of minutes	Retain for 3 years	Date of Meeting	Destroy	Common practice	
SCH 2.3	Agendas	No retention required	Conclusion of meeting	Destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 2.4	Reports	Retain at school for 6 years	Date of report	Transfer to ACET Record Office	Common practice	
SCH 2.5	Annual parents meeting papers	Retain at school for 6 years	Date of meeting	Transfer to ACET Record	Common practice	
SCH 2.6	Instrument of Government	Retain at school for the duration of its operation	Closure of school	Transfer to ACET Record	Common practice	
SCH 2.7	Trusts and Endowments	Retain at school whilst operationally required	End of operational use	Transfer to ACET Record	Common practice	
SCH 2.8	Action Plans	Retain for 3 years	Expiration of action plan	Destroy	Common practice	May be appropriate to offer to ACET Record Department
SCH 2.9	Policy documents	Retain while policy is used operationally	Expiration of policy	Transfer to archives when policy is no longer operational	Common practice	
SCH 2.10	Complaints files	Retain for 6 years	Resolution of complaint	Review and destroy if complaints are non-contentio	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
SCH 2.11	Annual reports required by central government	Retain at school for 10 years	End of the calendar year that the record was created in	Transfer to ACET Record Office	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	
SCHOOL MANAGEMENT						
SCH 3.1	Log books	Retain at school for 6 years	Date of last entry in log book	Transfer to ACET Record Office	Common practice	Legislation no longer requires the completion of a school log book
SCH 3.2	Minutes of management team	Retain at school for 5 years	Date of meeting	Transfer to ACET Record Office	Common practice	
SCH 3.3	Reports made by management team	Retain at school for 3 years	Date of report	Transfer to ACET Record Office	Common practice	
SCH 3.4	Development plans	Retain for 6 years	Expiry of plan	Review with a view to destroy	Common practice	May be appropriate offer to ACET Record Office Department
SCH 3.5	Successful school admissions applications	Retain for 1 year	Date of admission	Destroy	Common practice	

SCH 3.6	Unsuccessful school admission applications (where no appeal is made)	Retain for 1 year	Start of school term	Destroy	School Admissions Appeals Code 2012	
SCH 3.7	Unsuccessful school admission applications (where an appeal is made)	Retain for 1 year	Resolution of case	Destroy	School Admissions Appeals Code 2012	
SCH 3.8	Proofs of address supplied by parents as part of the admissions process	Retain for 1 year	Date of admission	Destroy	Common practice	
PUPIL RECORDS						
SCH 4.1	Admission registers	Retain for 6 years	Last entry in register	Transfer to ACET Record Office	Common practice	These are no longer created in paper format
SCH 4.2	Attendance registers	Retain for 3 years	Last entry in register	Destroy	Common practice	
SCH 4.3	Pupil files (primary school)	Retain for duration of the pupil's attendance at school	Date pupil changes school	Transfer to Secondary School	Common practice	In the case of school exclusions it may be appropriate to transfer to ACET Record Office
SCH 4.4	Pupil files (secondary school school)	Retain for 25 years	Pupil's date of birth	**Do not** destroy (refer to note on front page)	The Limitations Act 1980	

SCH 4.5	Special educational needs records relating to individual support provided by the schools (primary)	Retain for duration of attendance at school	Date pupil changes school	Transfer to Secondary School	Common practice	
SCH 4.6	Special educational needs records relating to individual support provided by the schools (secondary)	Retain for 35 years	Pupil's date of birth	**Do not** destroy (refer to note on front page)	Special Educational Needs and Disability Act 2001	This period is recommended by Derbyshire County Council.
SCH 4.7	Letters authorising	Retain for 2 years	Date of absence	Destroy	Common practice	
SCH 4.8	Public examination	Retain for 6 years	Date of examination	Destroy	Common practice	
SCH 4.9	Internal school examination	Retain for 5 years	Date of examination	Destroy	Common practice	
SCH 4.10	Advice and information issued by the school to parents regarding educational needs for individual	Retain for 12 years	Date advice issued	Destroy	Special Educational Needs and Disability Act 2001	
SCH 4.11	Accessibility Strategy	Retain for 12 years	Expiry of strategy	Destroy	Special Educational Needs and Disability Act 2001	May be appropriate to offer to ACET Record Office
SCH 4.12	Parental permission slips for school trips where there has not been a major incident	No retention required	Conclusion of trip	Destroy	Common practice	

SCH 4.13	Parental permission slips for school trips **where there has been a major incident**	Retain for 25 years from the date of birth of the pupil/s involved in the incident	Pupil's date of birth	Destroy	The Limitations Act 1980	
SCH 4.14	Records created by schools to obtain approval to run an Educational Visit outside the classroom where there has not been a major incident	Retain for 14 years	Date of visit	Destroy	The Health and Safety at Work Act 1974	Records created might include risk assessments
SCH 4.15	Records created by schools to obtain approval to run an Educational Visit outside the classroom **where there has been a major incident**	Retain for 21 years from the date of birth of the pupil/s involved in the incident	Pupil's date of birth	Destroy	The Limitations Act 1980	Records created might include risk assessments
SCH 4.16	Walking bus register	Retain for 3 years	Last entry in register	Destroy	Common practice	If there has been an incident it is assumed that an accident report will have been made and should be retained for the appropriate retention period (see Health and Safety section below)

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
CURRICULUM						
SCH 5.1	Curriculum development	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	
SCH 5.2	Curriculum returns	Retain for 3 years	End of the calendar year that the record was created in	Destroy	Common practice	
SCH 5.3	School syllabus	Retain for 1 year	Expiration of syllabus	Destroy	Common practice	May be appropriate to offer to ACET Record Office
SCH 5.4	Schemes of work	Retain for 1 year	End of the calendar year that the record was created in	Review with a view to destroy	Common practice	
SCH 5.5	Timetable development	Retain for 1 year	End of the calendar	Review with a view to destroy	Common practice	

			year that the record was created in			
SCH 5.6	Records of marks awarded	Retain for 1 year	End of the calendar year that the record was created in	Destroy	Common practice	
SCH 5.7	Records of homework set	Retain for 1 year	End of the calendar year that the record was created in	Destroy	Common practice	
PERSONNEL						
SCH 6.1	Staff personnel files	Retain for 7 years	End of employment	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.2	Interview notes for successful candidates	Retain and add to personnel file.			Common practice	
SCH 6.3	Interview notes for unsuccessful candidates	Retain for 6 months	Date successful candidate is in post	Destroy	Common practice	
SCH 6.4	Pre-employment vetting information (including DBS checks)	Retain for 6 months	Date information checked	Destroy	DBS guidelines	

SCH 6.5	Written warnings (level 1)	Retain for 6 months	Date of warning	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.6	Written warning (level 2)	Retain for 12 months	Date of warning	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.7	Final warning	Retain for 18 months	Date of warning	**Do not** destroy (refer to note on front page)	Common practice	
SCH 6.8	Warnings subsequently found to be based on an unfounded case (excluding child protection related warning)	No retention required	Date case found to be unfounded	**Do not** destroy (refer to note on front page)	Common practice	For child protection related warnings see Child Protection section above.
SCH 6.9	Staff appraisal records	Retain for 5 years	End of the calendar year that the record was created in	**Do not** destroy (refer to note on front page)	Common practice	
HEALTH AND SAFETY						
SCH 7.1	Accessibility Plans	Retain for 6 years	End of the calendar	Destroy	Disability and Equality Act 2010	
			year that the record was created in			
SCH 7.2	Accident/incident reporting	Retain for 7 years	Date of incident	Destroy	Common practice	

SCH 7.3	Accident/incident reporting	Retain for 25 years	Child's date of birth	Destroy	The Limitations Act 1980	
SCH 7.4	Records of monitoring areas where employees/pupils are likely to come into	Retain for 40 years	Last action on file	Destroy	The Control of Substances Hazardous to Health Regulations 2002	
SCH 7.5	Records of monitoring areas where employees/pupils are likely to come into	Retain for 50 years	Last action on file	Destroy	The Ionising Radiations Regulations 1985	
SCH 7.6	Fire log books	Retain for 7 years	End of calendar year	Destroy	Common practice	
SCH 7.7	Records of the administration of medicines for all routine medication (e.g. Calpol, antibiotics, treatments for asthma and diabetes)	Retain for 1 year	End of calendar year	Destroy	Business decision	Events significantly outside individual treatment plan should be treated as non-routine (see below)

SCH 7.8	Records of administration of medicines for all non-routine medication (e.g. peg feeding, epi-pen, invasive drugs, anti- depressants) and any records governing a reported incident, difficulty or issues with administering medication.	Retain for 21 years and 6 months from pupil's date of birth	Pupil's date of birth	Destroy	Business decision	
ADMINISTRATION						
SCH 8.1	Employer's Liability Certificate	Retain for 40 years	Closure of school		Common practice	Transfer to ACET Record Office on closure of school
SCH 8.2	Inventories of equipment/furnitu re	Retain for 6 years	End of calendar year	Destroy	Common practice	
SCH 8.3	Circulars to parents/staff/pup ils	Retain for 1 year	End of calendar year	Destroy	Common practice	
SCH 8.4	Newsletters produced by the school	Retain for 1 year	End of calendar year	Transfer to ACET Record	Common practice	
SCH 8.5	Visitor books	Retain for 2 years	End of calendar year	Destroy	Common practice	

Ref. No.	Functional Description	Retention Period	Trigger	Disposal action	Basis for retention	Comments
FINANCE						
SCH 9.1	Annual accounts	Retain at school for 6 years	End of calendar year	Transfer to ACET Record	Common practice	
SCH 9.2	Invoices, receipts, and other financial records covered by financial regulations	Retain for 6 years	End of calendar year	Destroy	Standard financial regulations	
SCH 9.3	Annual budget and supporting papers	Retain for 6 years	End of calendar year	Destroy	Common practice	
SCH 9.4	Ordinary contracts	Retain for 6 years	End of contract	Destroy	The Limitations Act 1980	
SCH 9.5	Contracts under seal	Retain for 12 years	End of contract	Destroy	The Limitations Act 1980	
PROPERTY						
SCH 10.1	Building plans	Retain whilst operational	End of operational use	Transfer to ACET Record	Common practice	
SCH 10.2	Burglary, theft and vandalism report forms	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	

SCH 10.3	Contractors' reports	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	
LOCAL AUTHORITY						
SCH 11.1	Secondary transfer sheets	Retain for 2 years	Year of	Destroy	Common practice	
SCH 11.2	Attendance returns	Retain for 1 year	End of the calendar year that the record was created in	Destroy	Common practice	
CENTRAL GOVERNMENT						
SCH 12.1	Major incident e.g Emergency Services, disease outbreak Ofsted reports and papers	Retain whilst current	Date new report issued	Transfer to ACET Record Office	Common practice	Replace old report with new report

SCH 12.2	Returns to central government	Retain for 6 years	End of the calendar year that the record was created in	Destroy	Common practice	